UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
EL PASO DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CAUSE NO. EP-11-CR-2728-KC-1**
	)	
ANGEL OCASIO	)	

REPLY TO GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO COMPEL PRODUCTION OF MATERIALS PERTAINING TO PEER-TO-PEER INVESTIGATIVE SOFTWARE

COMES NOW defendant ANGEL OCASIO (hereinafter "Mr. Ocasio"), by and through undersigned counsel, and files this Reply to Government's Response to Defendant's Motion to Compel Production of Materials Pertaining to Peer-to-Peer Investigative Software. In support thereof, he would respectfully show the following:

I. COPYRIGHT, TRADE SECRETS AND LAW ENFORCEMENT PRIVILEGE

Prior to addressing the individual responses to the request for production, it is worthwhile to clarify and distinguish three topics that pervade the affidavits and responses.

A copyright, by federal law through the Copyright Act of 1976, affords the original author or assignee certain rights, to include (1) reproduction of the copyrighted work in copies; (2) preparation of derivative works based upon the copyrighted work; (3) distribution of copies or phonorecords of the copyrighted work to the public by sale, or other transfer of ownership; or by rental, lease, or lending; (4) performance of the copyrighted work publicly, for example with a dramatic work; and (5) with sound recordings, the right to perform the copyrighted work publicly through digital transmission. *See* 17 U.S.C. § 106. These rights exist for one who (1) authors an original work and (2) fixes such work in any tangible medium of expression, now known or later developed, from which it can be perceived, reproduced, or otherwise communicated. *Id.* § 102.

"[T]he justification of the copyright law is the protection of the commercial interest of the artist/author. It is not to coddle artistic vanity or to protect secrecy, but to stimulate creation by protecting its rewards." *New Era Publications International, ApS v. Henry Holt & Co.*, 695 F. Supp. 1493, 1526 (S.D.N.Y. 1988). "The [author or assignee's] interest is, principally, a property interest in the copyrighted material." *Salinger v. Colting*, 607 F.3d 68, 81 (2d Cir. 2010) (citing *Wheaton v. Peters*, 33 U.S. 591, 661, 8 Pet. 591, 8 L.Ed. 1055 (1834)). In the context of this case, the use of open source peer-to-peer sharing software would not be subject to copyright protection as any use of this publicly available computer code would not be considered an original work. Copyright protection, to the extent it exists at all, would exist in original computer code added to the publicly available code, and would be limited to that original code.

In contrast to federal copyright law, State trade secret laws protect information that: (1) has an independent economic value as a result of its not being generally known and not readily ascertainable by proper means; and (2) is subject to reasonable efforts to maintain its secrecy. Unif. Trade Secrets Act § 1 (amended 1985), 14 U.L.A. 437 (1990); *see also Tewari De-Ox Systems, Inc. v. Mountain States/Rosen, L.L.C.*, 637 F.3d 604 (5th Cir. 2011)(applying Texas law in which trade secret status turns on (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of the information to the business and to its competitors; (5) the amount of effort or money expended in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others). Under trade secret law, computer code may qualify for trade secret protection. *See, e.g., Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 663 (4th

Cir. 1993).

Trade secret protection, which serves to deter improper disclosure of secret information, expires when the object of the protection is no longer a secret. *See, e.g., JustMed, Inc. v. Byce*, 600 F.3d 1118, 1128-30 (9th Cir. 2010). It is for this reason that courts routinely employ protective orders that prohibit the use or disclosure of information specific to trade secrets outside the bounds of the litigation. Unif. Trade Secrets Act § 5 (providing "a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval"). As was the case with the copyright illustration above, publicly available source code is, by definition, not a secret, thus may not be characterized as a protected trade secret. It is only when that source code is utilized in a unique and economically valuable manner that it may become a trade secret.

Finally, law enforcement officers and agencies may assert a law enforcement privilege or investigatory privilege "to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." *Commonwealth Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007). This privilege is qualified, and overcome by a demonstration of need. "When the information sought is both relevant and essential to the presentation of the case on the merits and the need for disclosure outweighs the need for secrecy, the privilege is overcome." *Miller v. Mehltretter*, 478 F. Supp. 2d 415, 424 (W.D.N.Y. 2007). In determining whether disclosure is

appropriate despite assertion of this privilege, the Fifth Circuit directs trial courts to consider the following factors:

> (1) the extent to which disclosure will thwart governmental processes by discouraging citizens from giving the government information; (2) the impact upon persons who have given information of having their identities disclosed; (3) the degree to which governmental self-evaluation and consequent program improvement will be chilled by disclosure; (4) whether the information sought is factual data or evaluative summary; (5) whether the party seeking discovery is an actual or potential defendant in any criminal proceeding either pending or reasonably likely to follow from the incident in question; (6) whether the police investigation has been completed; (7) whether any interdepartmental disciplinary proceedings have arisen or may arise from the investigation; (8) whether the plaintiff's suit is non-frivolous and brought in good faith; (9) whether the information sought is available through other discovery or from other sources; (10) the importance of the information sought to the plaintiff's case.

In re Dept. of Homeland Sec., 459 F.3d 565, 570 (5th Cir. 2006).

Given the degree to which these three concepts appear in the Government's Response, whether expressly or implicitly, it is hoped the foregoing sufficiently distinguishes the same for purposes of the following discussion.

II. THIRD PARTY POSSESSION

Counsel for the Government responds that the information sought in all but 2 of the discovery requests are held in the possession of a third party, a corporate entity. Resp. at 4. This answer is somewhat disingenuous, given the function of the software and the history of the affiant William Witse, as set forth in his affidavit.

As acknowledged in his affidavit, Mr. Wiltse is a former police officer from Oregon, and a present reserve police officer in Florida. Wiltse Aff. ¶ 1. He developed the peer-to-peer investigative software referred to as "Peer Spectre," which has evolved into the software now known as Child Protection Systems (CPS), *id.* ¶ 2, at issue in the present case.

CPS was developed by TRO, LLC, of Boca Raton, Florida, and Wiltse serves as the Director of Law Enforcement Programming at TRO. *Id.* Wiltse also regularly instructs law enforcement in the operation of CPS "prior to providing them access to the system." *Id.*

Much of the affidavit describing CPS suggests repetition of the the content of the search warrant affidavit, offered with additional nonspecific assurances such as "all components [of CPS] . . . function within the established protocols of the file sharing networks on which they operate," *id.* ¶ 6, "[e]very Gnutella message must adhere to a pre-defined structure . . . there is no way . . . to 'search' the . . . entirety of a computer's contents," *id.* ¶ 7, and "I am not aware of any problems affecting the reliability of data [CPS] collect[s]," *id.*

As this Court is already aware, and as stated in the search warrant affidavit, CPS permits the downloading of child pornography. If child pornography specific information, such as victim identities found in computer file names or actual child pornography computer files, are stored on the TRO network, then this company must be considered an agent of the federal government by contract or would be subject to criminal sanctions for violation of 18 U.S.C. § 3509, which restricts the handling of such material. *See id.* § 3509(m)(1)(providing "[i]n any criminal proceeding, any property or material that constitutes child pornography . . . shall remain in the care, custody, and control of either the Government or the court"). Wiltse is a current law enforcement officer specializing in the very area of law in which his software is now employed by federal agents. He asserts that the source code for CPS "has not been, and will not be, distributed" to any law enforcement agent or agency, Wiltse Aff. ¶ 10, presumably to avoid the problem of locally ordered court disclosure from agencies, which would come as no surprise if the operation of CPS and its programming is centrally located at TRO in Florida. Furthermore, given

the illegal nature of child pornography, it is difficult to conceive of how CPS would have value outside the realm of law enforcement agencies, which suggests a partnership in federal investigations which may not be avoided using the veil of a corporate entity. It therefore comes as no surprise that its corporate Internet site, http://www.tlo.com/, does not so much as offer a hint that might acknowledge the existence of CPS. If this were truly a commercial enterprise, as appears to be contended, rather than an outsourced investigator deputized as federal agent, then there would be no need to mask this product.

In *Dobyns v. E-Systems, Inc.*, 667 F.2d 1219 (5th Cir. 1982), the Fifth Circuit identified three possible theories on which a corporate entity could be characterized as a state actor, and therefore a partner with the federal government. The three theories identified are (1) "the government has so far insinuated itself into a position of interdependence (with a private entity) that it must be recognized as a joint participant in the challenged activity"; (2) the government has delegated a function "traditionally exclusively reserved to the State"; or (3) "there is a sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the state itself." *Id.* at 1221. By his own affidavit, which essentially relegates federal agents to mere pawns with regard to CPS in maintaining control of the system through a corporate account, Wiltse satisfies all three theories set forth above, and may not now claim a lack of involvement in accepting a traditional police power now entrusted to a corporate entity. Any claim of third party independence must be premised on blinders to the interdependence between federal agent and corporate entity in carrying out this

investigation.[1]

III. INFORMATION SOUGHT IS MATERIAL TO DEFENSE

The Indictment at issue in the present case alleges that Mr. Ocasio "knowingly receive[d] and attempt[ed] to receive" child pornography, and "knowingly distribute[d] and attempt[ed] to distribute" child pornography, in violation of 18 U.S.C. § 2252(a)(2). (Doc. No. 30; Counts One and 2). The affidavit offered in support of the search warrant application alleged that CPS, the subject of the present motion to compel, indicated that Mr. Ocasio's IP address "had downloaded . . . [specific] files associated with child pornography." De La Rosa Aff. ¶ 25. As stated throughout the proceedings on this Motion to Suppress, the only files specifically named and identified in this affidavit were not found on the computer seized in this case. If the Government's sole active detective measure in this case is established to be unreliable, as appears to be the case, and contrary to the Government's conclusory statement to the contrary, Resp. at 5, this evidence would significantly "alter the quantum of proof" in his favor. *United States v. Reeves*, 892 F.2d 1223, 1226 (5th Cir. 1990). As such, disclosure of the requested materials is warranted under Rule 16.[2]

---

[1]The Government suggests that the defense could "attempt to obtain" the material sought through a subpoena issued pursuant to Federal Rule of Criminal Procedure 17. Resp. at 4 n.1. As such an attempt would undoubtedly prompt a motion to quash arguing the same grounds the Government now advances, it is unclear how this approach resolves the present issue. As TLO is not a third party to this case, as contended by the Government, there is no need to proceed under the assumption that TLO is the equivalent of a telephone company when phone records are of evidentiary value.

[2]As discussed above, the Government's argument that the computer evidence sought is not within its "possession, custody, and control," Resp. at 6, rests on the theory that TLO's involvement is disassociated from the investigation. As TLO's involvement is inextricably linked to the actions of federal agents, it must be considered a federal agent. The software in its possession is therefore within the Government's "possession, custody, and control."

IV. INFORMATION SOUGHT IS MATERIAL TO MOTION TO SUPPRESS

The basis for materiality set forth above applies with equal force to an exercise of this Court's inherent authority as argued in the Motion to Compel. The Government has repeatedly been presented with the factual concern following forensic examination of the seized computer, specifically the absence of 3 files it elected to describe in detail based on its CPS examination, a fact confirmed by its own FTK Report, yet declines to explain the reason for this inconsistency. It chides the defense for its 'belief' that CPS operates outside the realm of this shared folder, Resp. at 7, yet offers no factual basis that might disprove this belief when it, and only it, has access to the system and materials in its possession that would serve to prove or disprove the same. It then turns to the conclusory statements offered by Wiltse as definitive proof that CPS operates within the limits of the law.

Counsel for the Government, having dealt with case after case involving CPS, herself appears to find the operation of CPS difficult to grasp. On page 2 of the Response to the Motion to Suppress, she declared Peer Spectre is "a completely separate and distinct computer system." Wiltse, in Paragraphs 2 and 6 of his affidavit, declares that Peer Spectre is a legacy component of CPS. Having exhibited an evident misunderstanding of CPS throughout these proceedings despite her access to the same, it would be understandable that the defense might not precisely define the system. Given the fact the defense has repeatedly associated Peer Spectre and CPS, the theory of Ms. Loehrs offered at the outset does not appear far from the mark in like of the Wiltse affidavit.

It is further worth noting that the affidavit offered by Wiltse in no way suggests any more than the representations of a corporate representative attempting to credit his product in the face

of possible scrutiny. He refers to his involvement in development of CPS, yet offers only generalities. Wiltse Aff. ¶ 2. There is nothing suggesting he is more than an advisor/project manager lacking specific understanding of the computer code or design of CPS. This lack of programming knowledge may suggest a "plausible deniability" approach in which he makes general requests and programmers design the code to meet and exceed peer-to-peer investigation requirements by any means necessary. If the Government believes programmers implement only the basic functionality required by project managers, then she would be wise to acquaint herself with the concept of programming "Easter eggs," which represent "an undocumented and often, unknown by management, key sequence that causes an application or game to do some thing it was not intended to do." Infinite Play, The Easter Egg Hunt (available at http://infiniteplaythemovie.com/EasterEggHunt.htm).[3] Absent some evidence that Wiltse has any computer programming experience that might permit him to actually know the operation of his product, rather than promote sales to law enforcement agencies and train on basic system operation as one might train a novice to use an e-mail program, the conclusory offerings of his affidavit are of little value in resolving the present Motion to Suppress.

The Government closes this portion of its Response, after acknowledging the warrantless search argument, Resp. at 6, by pointing out that undersigned counsel "elected to present no evidence" at the hearing. Resp. at 8. The reason for so doing was made abundantly clear, yet it bears noting that counsel for the Government, with possession of at least two items now sought,

---

[3]One well known example of an "Easter egg" is a flight simulator within the Microsoft Excel spreadsheet program that appeared when certain keys were pressed in sequence. The Spreadsheet Pages, Excel Easter Eggs (http://spreadsheetpage.com/index.php/oddity/excel_easter_eggs/).

elected to refrain from offering this evidence in her Response, despite the fact a warrantless search was alleged as incident to the *Franks* issue. It is respectfully submitted that the Government's repeated assertions that the defense cannot prove the system it controls itself justifies the order to compel production of the information now sought.

V. CPS MATERIALS WITHIN GOVERNMENT CONTROL

Separate and apart from the source code and CPS program itself, undersigned counsel requested written materials that may otherwise describe the program's operation. The Government responds that this material is the equivalent of a "report of examinations and tests" for purposes of Rule 16. Resp. at 10-11. As stated above, the concern is exclusively details of CPS operation, a tangible object, when alternative means of determining the same are lacking due to the Government's exclusive control. It is unclear how the Government draws its analogy, but it suffices to say that a description of software operation that might be found in a manual or training material, which lacks analytical value of any sort, cannot be considered a report of examination or test.[4]

VI. *BUDZIAK* IS INSTRUCTIVE

The Government contends that *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), is of little value as the investigative software in that case was developed by the FBI. Resp. at 12-15. As stated above, the fact that TLO is a corporate entity in this case and the FBI created the

[4]This Court is respectfully asked to note, after repeated demands for details of forensic testing, the Government's reliance on *United States v. Ashlock*, 105 Fed. Appx. 581, 586 (5th Cir. 2004), and its declaration that"Rule 16(a) does not instruct the government to provide detailed step-by-step information regarding the routine protocols employed by the expert in performing the tests discussed in the report."), and similar reliance on *United States v. Price*, 75 F.3d 1440 (10th Cir. 1996), and "ancillary requests," Resp. at 10-11, bearing a striking resemblance to its own requests for additional discovery with regard to the Motion to Suppress .

program in *Budziak* is, contrary to the Government's contention, a distinction without a difference. The fact that federal agents outsource an investigative requirement, and rely exceedingly on a corporate entity for round-the-clock investigative resources, inextricably links the two and effectively deputizes the corporate entity. Allowing the Government to claim private action would be akin to federal agents hiring private security to coerce confessions from suspects, then claiming private action and using the confessions at trial. TLO is a State actor, working in concert with federal agents on a continual basis. *Budziak* is therefore indistinguishable from the case at bar.

VII. LAW ENFORCEMENT PRIVILEGE DOES NOT PRECLUDE DISCLOSURE

The Government argues that disclosure would harm ongoing law enforcement operations, citing Paragraph 11 through 13 of the Wiltse affidavit. First, it bears noting that the private entity, TLO, appears to assert a law enforcement privilege itself. This should resolve any remaining doubts as to its degree of involvement in federal investigations. Second, as with trade secret issues described above, any concern directed to possible disclosure is easily resolved through a protective order. Counsel for the Government, while listing the perils of disclosure, fails to explain why a protective order limiting subsequent disclosure issued by this Court pursuant to its authority under Federal Rule of Criminal Procedure 16(d)(1) would not address the concerns. As this Court may readily protect these interests with the threat of contempt for violation of a non-disclosure order, the concerns identified by Wiltse and the Government are no impediment to an order compelling disclosure.

VIII. CONCLUSION

For the reasons set forth above, this Court is respectfully asked to grant the Motion to Compel in its entirety.

Very truly yours,

MAUREEN FRANCO
Federal Public Defender

/s/

MICHAEL GORMAN
Assistant Federal Public Defender
Western District of Texas
Federal Building
700 E. San Antonio, D-401
El Paso, Texas 79901
(915) 534-6525

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of April, 2013, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following: AUSA Brandy Gardes, Office of the U.S. Attorney, Richard C. White Federal Building, 700 E. San Antonio, Suite 200, El Paso, Texas.

/s/
Michael Gorman
Attorney for Defendant